SeaQuaKE: Sea-optimized Quantum Key Exchange

Technical Progress Report No. 2

Prepared for: Office of Naval Research
Contract #: N00014-14-C-0003
August 2014

Prepared by:
Paul Toliver, Principal Investigator
732-898-8146
ptoliver@appcomsci.com

Applied Communication Sciences

Drawing on its Telcordia, Bellcore and Bell Labs heritage, Applied Communication Sciences excels at creating innovative technologies and services to solve the most difficult and complex information and communications problems across commercial, carrier and government sectors. Applied Communication Sciences is legally registered as TT Government Solutions, doing business as Applied Communication Sciences. ACS operates as a standalone company under the corporate umbrella of its owner, The SI Organization, Inc.

REPORT DOCUMENTATION PAGE

FORM APPROVED
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED *(From - To)*
August 2014	Quarterly Technical Progress Report	June 2014 – August 2014

4. TITLE AND SUBTITLE

SeaQuaKE: Sea-optimized Quantum Key Exchange

Technical Progress Report No. 1

5a. CONTRACT NUMBER

N00014-14-C-0003

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Paul Toliver

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

TT Government Solutions (dba Applied Communication Sciences)
150 Mount Airy Road
Basking Ridge, NJ 07920-2021

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of Naval Research
875 North Randolph Street, Arlington VA 22203

DCMA Springfield
Bldg. 93, Picatinny Arsenal, NJ 07806-5000

10. SPONSOR/MONITOR'S ACRONYM(S)

ONR, DCMA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution Statement A. Approved for public release; distribution is unlimited

13. SUPPLEMENTARY NOTES

ONR-funded research: Special Notice 13-SN-0004 under ONRBAA13-001

14. ABSTRACT

This is the 2nd quarterly Technical Progress Report summarizing progress on the Sea-optimized Quantum Key Exchange (SeaQuaKE) project, which is led by Applied Communications Sciences under the ONR Free Space Optical Quantum Key Distribution Special Notice (13-SN-0004 under ONRBAA13-001).

In this technical report, we describe details of the hyperentanglement source architecture we propose for use in a maritime quantum communications system, including some of the wavelength-dependent considerations for technologies needed to construct such sources. In addition, we discuss initial simulation results using MODTRAN to model atmospheric transmission loss as a function of wavelength under a range of visibility conditions and aerosol model scenarios.

15. SUBJECT TERMS

Quantum communications, free-space optical communications

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	17. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
					Paul Toliver
a. REPORT	b. ABSTRACT	c. THIS PAGE	Same as report (SAR)	7	20. TELEPHONE NUMBER
Unclassified	Unclassified	Unclassified			(732) 898-8146

Table of Contents

1 Summary

This is the 2nd quarterly Technical Progress Report summarizing progress on the Sea-optimized Quantum Key Exchange (SeaQuaKE) project, which is led by Applied Communications Sciences under the ONR Free Space Optical Quantum Key Distribution Special Notice (13-SN-0004 under ONRBAA13-001).

In this technical report, we describe details of the hyperentanglement source architecture we propose for use in a maritime quantum communications system, including some of the wavelength-dependent considerations for technologies needed to construct such sources. In addition, we discuss initial simulation results using MODTRAN to model atmospheric transmission loss as a function of wavelength under a range of visibility conditions and aerosol model scenarios.

2 Introduction

The objective of the ONR SeaQuaKE project is to optimize the performance of free-space optical (FSO) quantum key distribution (QKD) operating under challenging maritime atmospheric conditions. In particular, a modeling framework will be developed to guide optimization of the *system operating wavelength* in order to maximize throughput and/or transmission distance over a wide range of atmospheric conditions. The framework will consider the major components of the quantum communication system including the transmitter, quantum channel, and receiver elements. Applied Communication Sciences (ACS) will focus its efforts on the transmitter and receiver elements, while Stevens Institute of Technology (SIT) will focus their effort on the free-space channel.

The focus areas over the last quarter include (i) further development of the hyperentanglement transmitter architecture and its wavelength dependencies and (ii) modeling transmission loss of the atmospheric free-space channel. These two technical areas are being led by ACS and SIT, respectively. Progress towards developing models for these elements in the quantum communications system is described below.

3 Methods, Assumptions and Procedures

3.1 Source Architecture and Modeling

The transmitter in our system will be hyperentanglement-based in order to enable greater system throughput. We will consider polarization and time-bin for the entanglement degrees of freedom due to superior channel characteristics for these modes as well as good coupling into and out of single mode fibers. The focus of our source effort is to understand the critical components and key performance parameters that vary as a function of system operating wavelength. We focus our efforts on 5 infrared wavelength bands with the best transmissivity through the atmosphere: 0.8, 1.3, 1.5, 3.5, and 9 μm.

The hyperentanglement source can be broken down into three smaller subsystems, including the pump source, time-bin multiplexer, polarization entanglement & pair generation elements. The approach we are taking is to survey the current body of literature on these sub-systems to understand state-of-the-art performance capabilities, trends towards improved performance, as well as fundamentals limits of specific enabling technologies. It will be critically important to understand how each of these factors varies as a function of source operating wavelength. Ultimately, these factors will translate to a range of higher-level source metrics to be considered in our model including entanglement quality, pair probability, pulse rate, mode quality, and signal-to-noise ratios.

3.2 Channel Model and Validation

The channel consists of the free-space link separating the transmitter and receiver elements of the quantum communications systems. We are assuming the quantum signal may propagate through a challenging maritime environment with widely variable atmospheric conditions including haze, fog, clouds, and rain, as well as scattering and turbulence effects. We will also be considering additional sources of noise that can corrupt the quantum signal recovered at the receiver, including noise introduced by sunlight as well as blackbody radiation.

The first channel impairment we have started to consider through modeling is atmospheric propagation loss. SIT has set up an initial MODTRAN simulation for atmospheric transmission modeling based on version 5.2.1 of the software. The atmospheric profile selected in MODTRAN defines the temperature and ratio of major gases and particles assumed in the simulation, which include, for example, H_2O, O_2, CO, CO_2, and N_2O. The U.S. standard atmospheric profile was used in the simulations, where the mixing ratio of major gases is illustrated below:

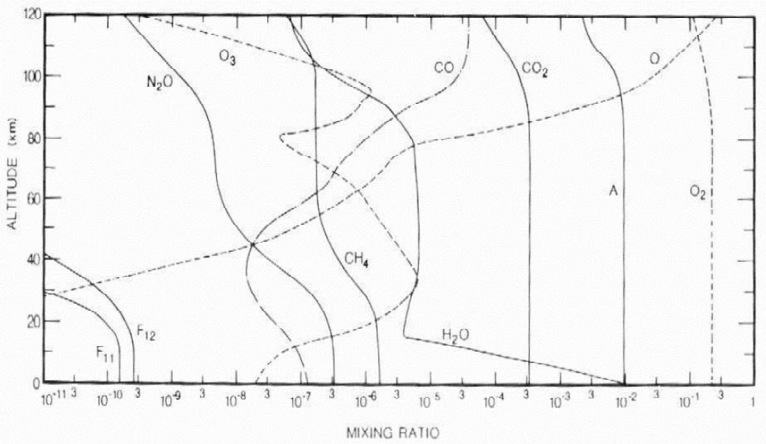

Figure 1. Mixing ratio of major gases for U.S. Standard atmospheric profile in MODTRAN.

Up to 5 different aerosol models were considered in the atmospheric transmission simulations, including (i) Navy Maritime, (ii) Maritime, (iii) Rural, (iv) Urban, and (v) Troposphere. As an example, the particles distribution for the Navy Aerosol Model is provided below:

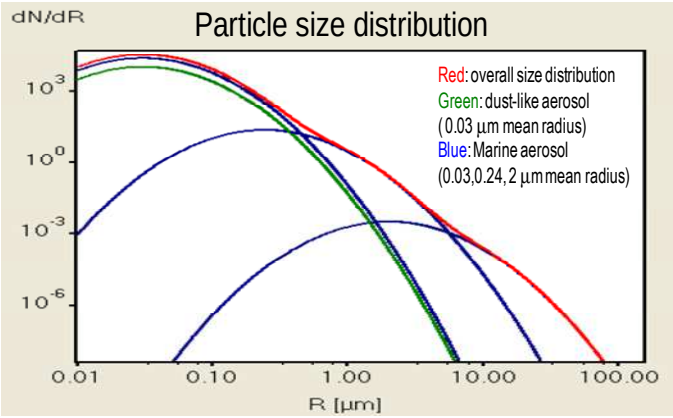

Figure 2. Particle size distribution for Navy Aerosol Model in MODTRAN.

MODTRAN simulations were performed over a 1-10 μm wavelength range (with 0.1, 1, 5, 15 cm^{-1} resolution) assuming a 30 km free-space link distance at an altitude of 10 m. The effective visibility was varied from 5 km to 50 km by scaling the particle size distribution appropriately. Additional MODTRAN simulation parameters included assuming a relative humidity of 50% and a wind speed=5 m/s.

.

4 Results and Discussion

4.1 Source Architecture and Modeling

We have begun our source model evaluations by considering the architecture given below in Figure 3. The hyperentangled source is broken down into several sub-systems including the pulsed optical pump, the time-bin interferometer, and the $\chi^{(3)}$ containing fiber loop which generates the single photon pairs. This architecture is based on fiber-based components and connections. Optical fiber interconnects are relatively stable and maintain the photon pairs in a single spatial mode, which is critical for ideal propagation through the atmosphere. $\chi^{(3)}$ materials are chosen initially due to their established ability to be integrated with single mode fiber and the ease with which they can be utilized for spontaneous four-wave mixing. We anticipate, however, that our future efforts will also include other types of nonlinear materials.

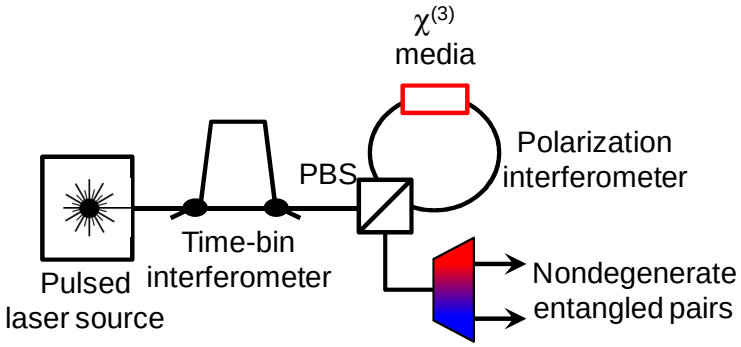

Figure 3 Source model architecture for generating hyperentangled photon pairs. Sub-systems will be chosen and evaluated in terms of meeting the source metrics stated in the text.

Our efforts this quarter have focused on the identification of ideal optical pump sources, which will ultimately drive the nonlinearity which produces the single photon pairs. We have identified several critical parameters which must be satisfied by the pump so that the desired quantum communication rates and distances can be realized. These are summarized below in Table 1.

Table 1. Pump Parameters

Parameter	Value
Pulse Rate	1 GHz
Time-bin Separation	<500 ps
Pulse FWHM	10-100 ps
Peak Power	~1 W

A pulse rate of 1 GHz is chosen because we anticipate it can be reasonably met with currently available technology, though depending on channel characteristics and detector efficiencies, higher pulse rates may have to be used to boost key rates. This pulse rate then dictates the requirements for the time-bin separation (< ½ pulse period) and the pulse temporal full-width half-maximum (FWHM) so that there is no pulse field overlap at the output of the source. Finally, the pulse source must be capable of outputting sufficient peak powers to drive the nonlinearity hard enough to maintain sufficient pair production probabilities, μ. High μ will

ensure good key rates, though a limit of approximately 0.01 is typically assumed in entanglement-based QKD systems in order to prevent photon splitting attacks. In 1550 nm systems employing dispersion-shifted fiber it is known that $\mu \propto (\gamma PL)^2$ and γL ~ 0.1 is a reasonable estimate. This implies that a peak power of ~ 1 W should be adequate for producing ideal photon pair rates. This power level is used as a starting point for evaluating the various technological options currently available for optical pumps. Finally, our initial technology survey is focusing on self-pulsing sources, such as mode-locked lasers (MLL), due to low complexity and high peak powers. MLL powers are sufficiently high that filtering to appropriate pulse widths and or passive temporal multiplexing to GHz rates is possible. The first step in establishing the system model is ensuring that technologies are available in the wavelength bands of interest which are capable of meeting the metrics outlined in Table 1. Our current results are summarized below in Table 2. Many of these options are commercially available, while others are likely to require additional technology development efforts.

Table 2. Pump Technologies

Wavelength (μm)	MLL Options
0.8	Er + SHG, Ti:Sa
1.3	Pr, OPO
1.5	Er:glass
3.5	HoPr:ZBLAN
9	QCL, Er+DFG

Table 2 acronyms: OPO = optical parametric oscillator, Er = erbium, SHG = second harmonic generation, Ti:Sa = titanium sapphire, Pr = praseodymium, Ho = holmium, ZBLAN = a family of fluoride glasses, QCL=quantum cascade laser, DFG=difference frequency generation

4.2 Channel Model and Validation

The results of the MODTRAN simulation of transmissivity for a 30 km free-space link assuming a Navy Maritime aerosol model, U.S. standard atmosphere, along with additional simulation parameters defined early in Section 3.2 is shown in Figure 4. Under high visibility conditions (e.g. 23, 50 km), reasonably good transmittance can be seen in 1.5-2 μm, 2-2.5 μm, 3.5-4 μm, and 8-10 μm wavelength regions. However, as visibility is reduced (e.g. 5, 10 km), these preliminary simulations results suggest significantly lower loss at longer wavelengths, with almost 5 orders of magnitude increase in the calculated transmittance at 10 μm vs. 1.5 μm when visibility is 5 km.

In order to explore the sensitivity of atmospheric transmission to different aerosol distributions, MODTRAN simulations were performed using a range of aerosol models including (i) Navy Maritime, (ii) Maritime, (iii) Rural, (iv) Urban, and (v) Troposphere. Simulations of both low visibility (e.g. 5 km) and higher visibility conditions (e.g. 23 km) were performed, and the results are shown in Figure 1. As in the Navy Maritime environment, there is a general trend towards reduced transmissivity, particularly at shorter wavelengths (e.g. 1 μm), when visibility is reduced.

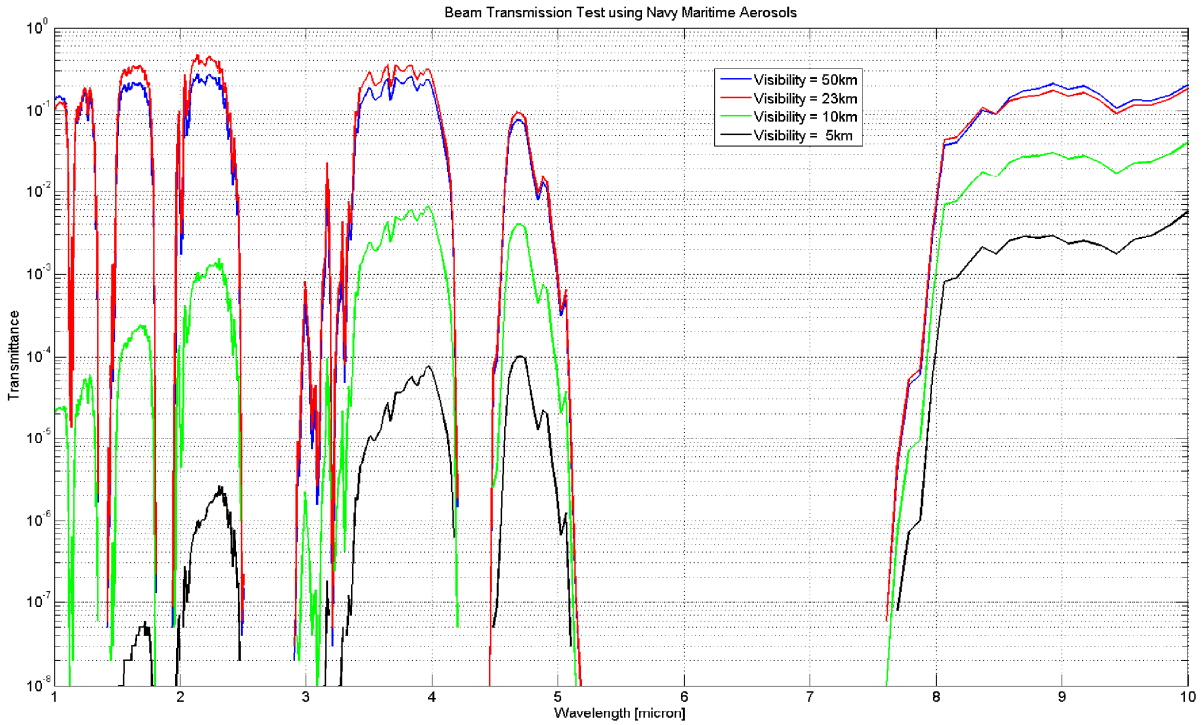

Figure 4. MODTRAN atmospheric simulation of 30 km free-space link with different visibility levels. (Navy Maritime aerosol model, U.S. standard atmosphere, additional simulation parameters defined in Section 3.2)

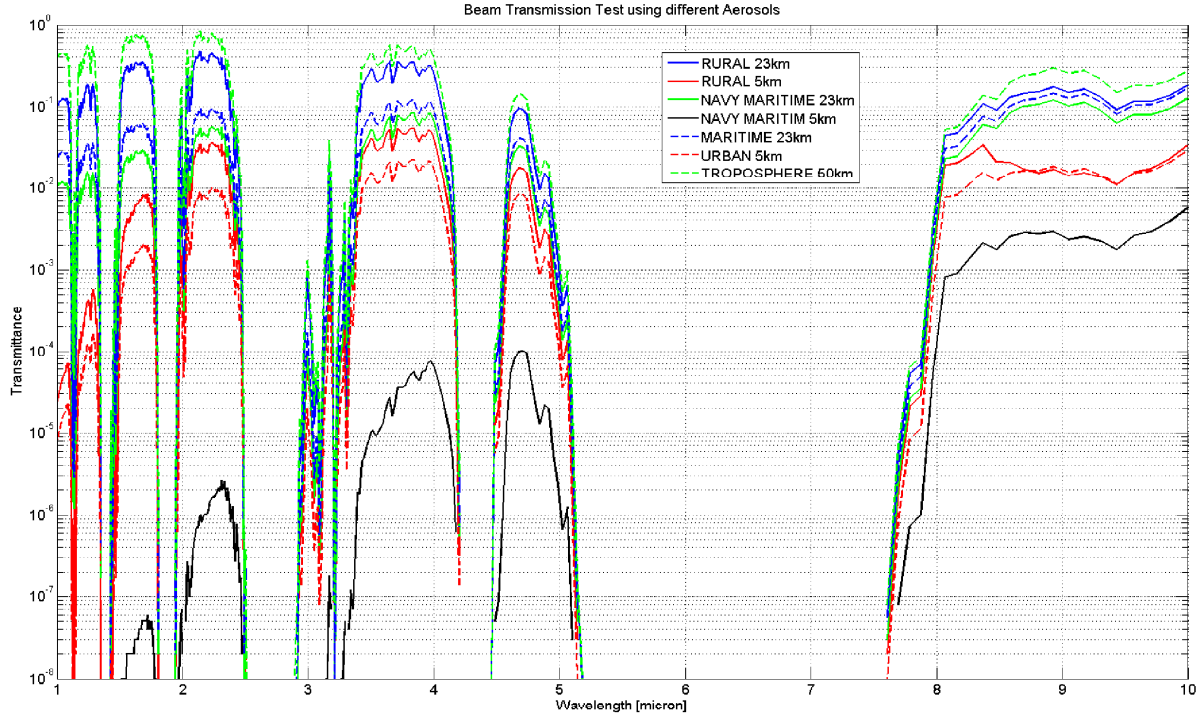

Figure 5. MODTRAN atmospheric simulation of 30 km free-space link with different visibility levels and different aerosol models. (U.S. standard atmosphere, additional simulation parameters defined in Section 3.2)

4.3 Deliverables/Milestones

Date	Deliverable/Milestone	Status
June 2014	Progress Report No. 1: Year 1, 1st Quarter	✓
August 2014	Progress Report No. 2: Year 1, 2nd Quarter	✓
November 2014	Progress Report No. 3: Year 1, 3rd Quarter	
February 2015	Progress Report No. 4: Year 1, 4th Quarter	
May 2015	Progress Report No. 5: Year 2, 1st Quarter	
August 2015	Progress Report No. 6: Year 2, 2nd Quarter	
November 2015	Progress Report No. 7: Year 2, 3rd Quarter	
February 2016	Progress Report No. 8: Year 2, 4th Quarter	
May 2016	Progress Report No. 9: Year 3, 1st Quarter	
August 2016	Progress Report No. 10: Year 3, 2nd Quarter	
November 2016	Progress Report No. 11: Year 3, 3rd Quarter	
February 2017	Final Report	

5 Conclusions

In the last quarter of the SeaQuaKE project, ACS has gone into further design of the hyperentanglement source architecture and the requirements on the associated technologies that would allow it to operate at different free-space transmission bands from 0.8 μm to 10 μm. In addition, SIT has initiated MODTRAN simulations that point to substantial benefits of operating in MWIR and LWIR bands under low visibility conditions. Finally, we attended an ONR program review, which was held at Sandia on July 22-23, 2014. No problems are currently anticipated.